École normale supérieure
MPRI, M2, 2.6

Cours "Interprétation abstraite : application à la vérification et à l'analyse statique"

Examen du 2 décembre 2005

8h45 – 11h45, salle U/V

Le but de l'examen est d'étudier la notion de complétude en interprétation abstraite.

Soit $\langle C, \leq, \bot, \top, \vee, \wedge \rangle$ un treillis complet. Les abstractions de C sont les images $\mu(C)$ par une fermeture supérieure μ sur C, $\mu \in \underline{uco}(C)$, où d'après Ward, $\langle \underline{uco}(C), \dot{\leqslant}, \lambda x.\, x, \lambda x.\, \top, \dot{\sqcup}, \dot{\wedge} \rangle$ est un treillis complet avec $\rho \dot{\leqslant} \eta$ si et seulement si $\forall x \in C : \rho(x) \leqslant \eta(x)$, $(\dot{\bigwedge_i} \rho_i)(x) = \bigwedge_i (\rho_i(x))$ et $(\dot{\bigsqcup_{i \in \Delta}} \rho_i)(x) = x$ ssi $\forall i \in \Delta : \rho_i(x) = x$. On rappelle que $\underline{uco}(C)$ est complètement déterminé par ses points fixes $\rho(C) = \{x \in C \mid \rho(x) = x\}$ et $\rho \dot{\leqslant} \eta$ ssi $\eta(C) \subseteq \rho(C)$ où $f(X) = \{f(x) \mid x \in X\}$ est l'image de l'ensemble X par la fonction f. Dans la suite si $\rho \in \underline{uco}(C)$, on notera $\rho(C)$ simplement par ρ. On note $\mathcal{M}(X) = \{\wedge Y \mid Y \subseteq X\}$ la plus petite famille de Moore contenant X ($\top \in \mathcal{M}(X)$). On notera également $\mathcal{M}(X)$ l'opérateur de fermeture supérieure ayant $\mathcal{M}(X)$ comme points fixes. On a $\dot{\bigsqcup_{i \in \Delta}} \rho_i = \mathcal{M}(\bigvee_{i \in \Delta} \rho_i)$.

Question 1

Soit $\langle C, \leq \rangle$ un treillis complet, $\rho \in \underline{uco}(C)$ et $X \subseteq C$. Montrer que :

$$\rho(\wedge \rho(X)) = \rho(\wedge X)$$

$\square$

Soit $f \in C \xrightarrow{m} C$ un opérateur monotone (ou croissant) sur C ($x \leq y$ implique $f(x) \leq f(y)$). Soit $f^\#$ une abstraction de f pour $\langle C, \leq \rangle \underset{\mu}{\overset{1}{\leftrightarrows}} \langle \mu(C), \leq \rangle$ où $1 = \lambda x . x$ est l'identité

- $f^\#$ est dite <u>correcte</u> ssi $\mu \circ f \dot{\leq} f^\# \circ \mu$
- $f^\#$ est dite <u>complète</u> ssi $f^\# \circ \mu \dot{\leq} \mu \circ f$
- la <u>meilleure abstraction</u> $\hat{f}$ de f est $\hat{f} = \mu \circ f \circ 1$ $= \mu \circ f$.

Question 2

Démontrer que si $f \in C \xrightarrow{m} C$ est croissante alors $\hat{f} \in \mu(C) \to \mu(C)$ est correcte et $\hat{f} = \mu \circ f \circ \mu$

Question 3

Démontrer qu'il est possible de définir une abstraction correcte et complète $f^\#$ de $f \in C \xrightarrow{m} C$ sur $\mu(C)$, $\mu \in \underline{uco}(C)$ si et seulement si $\hat{f}$ est complète (soit $\mu \circ f \circ \mu \leq \mu \circ f$).

La condition $\mu \circ f = \mu \circ f \circ \mu$ est donc une condition suffisante de correction et de complétude de l'abstraction de points fixes comme le montre la question suivante.

Question 4

Soit $\langle C, \leq \rangle$ un treillis complet, $f \in C \xrightarrow{m} C$ croissante, $\mu \in \underline{uco}(C)$ tel que $\mu \circ f = \mu \circ f \circ \mu$.
Démontrer que $\mu(\mathrm{lfp}\, f) = \mathrm{lfp}(\mu \circ f)$ $\square$

On admettra dans les démonstrations le principe de chaine maximale de Hausdorff, à savoir que toute chaîne croissante dans un ensemble partiellement ordonné $\langle P, \leq \rangle$ peut être étendue en une chaîne maximale. Si $X \subseteq P$. On note $\underline{\max}(X)$ l'ensemble des elements maximaux de X.

Question 5

Donner un exemple C, f pour lequel $\hat{f}$ n'est pas complète.

Si $\hat{f}$ n'est pas complète, c'est que le domaine abstrait $\mu(C)$ est trop ou pas assez abstrait pour qu'il soit possible de calculer l'image abstraite d'une propriété $P \in C$ par f sans perte irrémediable d'information quand cette propriété est abstraite. Dans ce cas, on peut raffiner le domaine abstrait $\mu(C)$ (à la limite, l'identité est complète) ou abstraire $\mu(C)$ (à la limite $\lambda P. \top$ est complète). En fait, pour f donné, il existe un domaine abstrait le plus abstrait et un le plus concret pour lesquels $\hat{f}$ est complet pour ces domaines question 6

Soit $\{\mu_\gamma \mid \gamma < \lambda\}$ une famille de domaines abstraits $\mu_\gamma(C)$ sur le Treillis complet $\langle C, \leq \rangle$ qui sont corrects et complets pour $f \in C \xrightarrow{m} C$. Démontrer que $\dot{\bigsqcup}_{\gamma<\lambda} \mu_\gamma$ et $\dot{\bigwedge}_{\gamma<\lambda} \mu_\gamma$ sont complets pour f (où les bornes supérieures et inférieures sont comprises dans $\underline{uco}(C)$). $\square$

Une fonction $f \in C \to C$ est continue au sens de Scott si et seulement si pour toute chaine croissante X de C on a $f(\vee X) = \vee f(X)$ ou $f(X) = \{f(x) \mid x \in X\}$ et $\vee Z$ denote la borne supérieure de $Z \subseteq C$ dans $\langle C, \leq \rangle$ si elle existe.

question 7

Soit $f \in C \xrightarrow{c} C$ continue au sens de Scott et $y \in C$. Démontrer que si $f(x) \leq y$ alors il existe $z \in \underline{max}\{x \mid f(x) \leq y\}$ tel que $x \leq z$. $\square$

Dans la suite on généralise la condition de complétude $\mu \circ f = \mu \circ f \circ \mu$ à

$$\eta \circ f = \eta \circ f \circ \rho$$

où $f \in C \xrightarrow{m} C$ et $\eta, \rho \in \underline{uco}(C)$. On pose :

$$\Gamma(C, f) = \{\langle \rho, \eta \rangle \mid \eta \circ f = \eta \circ f \circ \rho\}$$

question 8

soit $f \in C \to C$ continue au sens de Scott, $\rho, \jmath \in \underline{uco}(C)$. Demontrer que

$$\jmath \circ f = \jmath \circ f \circ \rho$$

$\iff$

$$\bigcup_{y \in \jmath(C)} \underline{\max}\{x \in C \mid f(x) \leq y\} \subseteq \rho(C)$$

question 9

soit $f \in C \to C$ continue au sens de Scott, $\rho, \jmath \in \underline{uco}(C)$. Démontrer qu'il existe $\zeta \in \underline{uco}(C)$ tel que

$$\zeta(C) = \{y \in C \mid \underline{\max}\{x \in C \mid f(x) \leq y\} \subseteq \rho(C)\}$$

En donnée $f \in C \to C$ continue, on pose

$$\mathcal{F}_f(\rho) = \zeta$$

tel que

$$\zeta(C) = \{y \in C \mid \underline{\max}\{x \in C \mid f(x) \leq y\} \subseteq \rho(C)\}.$$

question 10

Démontrer que $\jmath \circ f = \jmath \circ f \circ \rho \iff \mathcal{F}_f(\rho) \sqsubseteq \jmath$, (où l'ordre $\sqsubseteq$ est le même que $\leqslant$ utilisé dans les questions précédentes).

Etant donné un treillis complet $\langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap \rangle$, $f \in L \to L$ croissant et $x \in L$, on note $\mathrm{lfp}_x^{\sqsubseteq} f$ le plus petit point fixe de f qui est $\sqsubseteq$-superieur ou égal à x.

Question 11

Etant données $f \in C \to C$ continue et $\rho \in \underline{uco}(C)$, on pose :

$$\eta = \mathrm{lfp}_{\rho}^{\sqsubseteq} \mathcal{F}_f$$

Montrer que η existe et satisfait :

($\underline{1}$) $\rho \sqsubseteq \eta$

($\underline{2}$) $\eta \circ f \circ \eta = \eta \circ f$

($\underline{3}$) si $\eta' \circ f \circ \eta' = \eta' \circ f$ et $\eta' \sqsupseteq \rho$ alors $\eta \sqsubseteq \eta'$

($\underline{4}$) $\eta \circ f \circ \rho = \eta \circ f$

Autrement dit η est l'abstraction qui abstrait ρ (1), qui est complète pour f (2) et qui est la plus raffinée possible ayant cette propriété ($\underline{3}$).

On pose maintenant. $\mathcal{G}_f(\eta) = \xi \in \underline{uco}(C)$ tel que

$$\xi(c) = \mathcal{M}\left(\bigcup_{y \in \eta(c)} \underline{\max}\{x \in C \mid f(x) \leq y\}\right)$$

où $\mathcal{M}(Y) = \{\wedge X \mid X \subseteq Y\}$ (donc $\top \in \mathcal{M}(Y)$) est la famille de Moore engendrée par Y.

question 12 :

Démontrer que l'on a une correspondance de Galois :

$$\langle \underline{uco}(C), \sqsubseteq \rangle \underset{\alpha_f}{\overset{G_f}{\leftrightarrows}} \langle \underline{uco}(C), \sqsubseteq \rangle$$

(où f continue).

question 13

Etant donnés $f \in C \to C$ continue et $\rho \in \underline{uco}(C)$

On pose $\quad \eta = \mathrm{gfp}_\rho^{\sqsubseteq}\, G_f$

Montrer que η existe et satisfait :

(1) $\eta \sqsubseteq \rho$

(2) $\eta \circ f \circ \eta = \eta \circ f$

(3) si $\eta' \circ f \circ \eta' = \eta' \circ f$ et $\eta' \sqsubseteq \rho'$ alors $\eta' \sqsubseteq \eta$

Autrement dit η est l'abstraction qui raffine ρ, qui est complète pour f et qui est la plus abstraite possible ayant cette propriété.

Quand f n'est pas complète sur ρ on peut donc abstraire ρ (question 11) ou raffiner ρ (question 13) pour obtenir une abstraction complète pour f.

Une autre définition de la complétude (qui correspond à $f \circ \gamma = \gamma \circ f^{\#}$, qui n'est pas equivalent à $\alpha \circ f^{\#} = f \circ \alpha$) est $f \circ \mu = \mu \circ f \circ \mu$.

Question 14

Soit $f \in \wp(C) \xrightarrow{m} \wp(C)$ croissante (monotone) pour $\subseteq$ et $\mu \in \underline{uco}(\wp(C))$. Démontrer que

$$\mu \circ f = \mu \circ f \circ \mu$$
$$\Leftrightarrow \quad \forall S \in \wp(Q) : \forall T \in \mu : f(S) \subseteq T \Leftrightarrow f(\mu(S)) \subseteq T$$

On peut donc maintenant démontrer que

Question 15

Soit $f \in \wp(C) \xrightarrow{m} \wp(C)$ croissante et $\mu \in \underline{uco}(\wp(C))$. On a :

$$\mu \circ f = \mu \circ f \circ \mu$$
$$\Leftrightarrow \forall h \in \wp(Q) \to \wp(Q)$$
$$[[\forall X \in \wp(Q) : f(h(X)) \subseteq X] \wedge \left[\begin{array}{c} h \text{ maximal} \\ \text{ayant cette propriété} \end{array}\right]]$$
$$\Rightarrow h \circ \mu = \mu \circ h \circ \mu$$

$\wr$